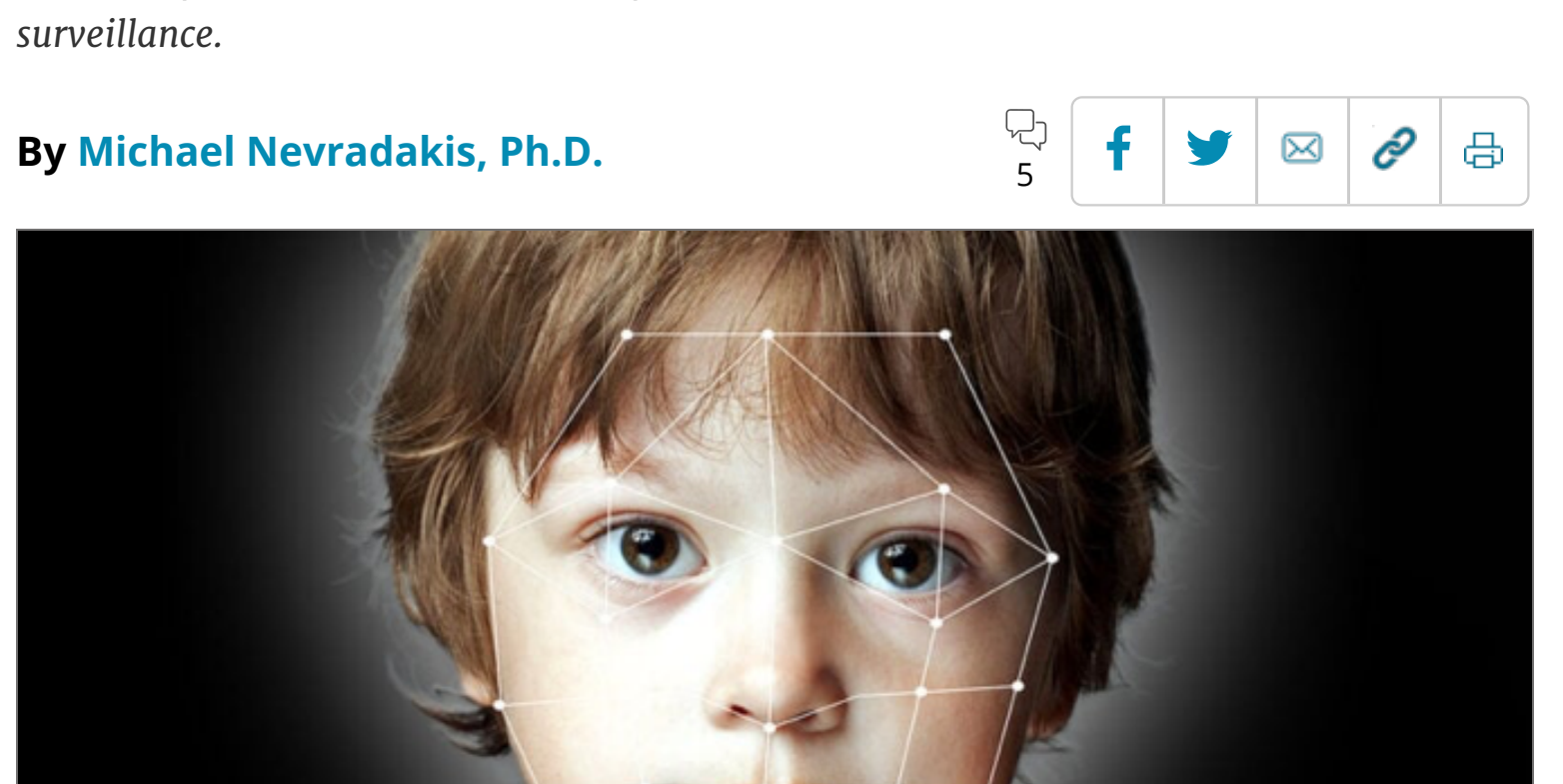
08/02/23 • BIG TECH › NEWS

Critics Sound Alarm as FTC Weighs Gaming Industry Proposal to Verify Parental Consent Using Facial Age-Verification Technology

The Federal Trade Commission is considering a proposal to allow businesses to use facial biometric scanning "age-estimation technology" to obtain parental permission for children under 13 to use online gaming services, but critics say the technology opens the door to collecting private data — on kids and parents — and risks normalizing biometric surveillance.

By **Michael Nevradakis, Ph.D.**

5



Miss a day, miss a lot. *Subscribe to The Defender's Top News of the Day.* ***It's free.***

The Federal Trade Commission (FTC) is considering a proposal that would allow businesses to use facial biometric scanning "age-estimation technology" to obtain parental permission for children under 13 to use online gaming services.

Yoti, a digital identity (ID) company, along with Epic Games, a subsidiary of the parental-consent management firm SuperAwesome, and the Entertainment Software Rating Board (ESRB) submitted the proposal.

They are requesting approval for "Privacy-Protective Facial Age Estimation" technology under the Children's Online Privacy Protection Act (COPPA).

Under COPPA, online sites and services "directed to children under 13" must obtain parental consent before collecting or using personal information from a child.

The law includes several "acceptable methods for gaining parental consent" and provisions "allowing interested parties to submit new verifiable parental consent methods" for approval.

The FTC's public comment period for the proposal ends Aug. 21.

The companies backing the proposal claim the technology obtains only portions of a facial image and the data are immediately deleted once the verification process has been completed.

However, privacy activists who spoke with The Defender said the proposal does not sufficiently address a number of privacy concerns associated with the technology.

Some experts also raised questions about the implications and potential misuses of facial recognition technology more broadly.

RFK Jr./Hooker NEW book: Vax-Unvax. Order Now!

Not as accurate as claimed?

"Privacy-Protective Facial Age Estimation" technology "analyzes the geometry of a user's face to confirm that they are an adult," according to the FTC.

According to the proposal submitted by the three applicants:

> "Privacy-Protective Facial Age Estimation provides an accurate, reliable, accessible, fast, simple and privacy-preserving mechanism for ensuring that the person providing consent is the child's parent."

The proposal compares the technology to existing verification methods:

> "Facial age estimation uses computer vision and machine learning technology to estimate a person's age based on analysis of patterns in an image of their face. The system takes a facial image, converts it into numbers, and compares those numbers to patterns in its training dataset that are associated with known ages.
>
> "By contrast, facial recognition technology, which seeks to identify a specific person based on a photo, looks for unique geometric measures of the face, such as the distance and relationship among facial features, and tries to match these to an existing unique set of measurements already recorded in a database along with unique identifying information."

The applicants said their proposed technology draws upon a "neural network model by feeding it millions of images of diverse human faces with their actual month and year of birth."

"The system converts the pixels of these images into mathematical functions that represent patterns. Over time, the system has learned to correlate those patterns with the known age," the applicants stated.

Citing a Yoti white paper, the proposal explains how these images are then processed:

> "When performing a new age estimation, the system extracts the portions of the image containing a face, and only those portions of the image are analyzed for matching patterns.
>
> "To match patterns, each node in Yoti's neural network performs a mathematical function on the pixel data and passes the result on to nodes in the next layer, until a number finally emerges on the other side. The only inputs are pixels of the face in the image, and the only outputs are numbers. Based on a review of the number patterns, the system creates an age estimation."

According to the proposal, the user takes a photo of themselves (a selfie) assisted by an "auto face capture module" that guides the positioning of their face in the frame. The system then checks whether there is a live human face in the frame and requires the image to be captured in the moment.

The system doesn't accept still images, and photos that don't meet the quality requirements are rejected. "These factors minimize the risk of circumvention and of children taking images of unaware adults," according to the proposal.

Julie Dawson, chief policy and regulatory officer for Yoti, told Biometric Update the software "is privacy-preserving, accurate, and easier to use by more parents" compared to existing alternatives.

"In addition, we have completed over four million age estimations for SuperAwesome outside the U.S. — a sign of its popularity among parents. Where facial age estimation is available as an option for parental consent outside the U.S., more than 70 percent of parents choose it over other methods," she stated.

According to Biometric Update, "SuperAwesome and Yoti have worked together on the software and began marketing it outside the U.S., beginning last year. … It's reportedly 99.97 percent accurate in identifying an adult."

But the companies also concede that "a third of people in the European Union and the United Kingdom to date have been blocked by facial age estimation," leading to questions about the true accuracy of the technology.

And a February 2022 Sifted article states that the technology "is usually able to accurately estimate age to within a four to six-year range," and "as recently as 2018, the accuracy wasn't where it should be on darker skin tones."

Anonymity 'would be utterly eradicated'

According to SuperAwesome's website, the "Personally identifiable information" collected by the technology "includes name, address, geolocation, email address or other contact information, user-generated text or photo/video, and persistent identifiers (like device IDs and IP addresses), many of which are necessary for basic product features."

Despite assurances that no personal information is collected, just portions of one's facial image, and that the data are immediately deleted, the website also states:

> "To deliver great online experiences for young audiences, many digital services — including games, educational platforms, and social communities — benefit from the use of personal information to power key features or to enable personalization."

What appears to be unaddressed by these statements is the possibility that children may attempt to use the age verification system anyway, in addition to the possibility that whatever images are collected could nevertheless be connected to other personal information entered by children or parents as part of an online registration or purchase.

It also is unclear how the software, aside from verifying that the individual whose face is being scanned is an adult, can confirm that they are also a parent or legal guardian of that child, and not some other unrelated individual.

Privacy and legal experts who spoke with The Defender wondered how personally identifiable information, as well as IP addresses and geolocation data, might be collected, despite assurances to the contrary, and how that information might be used, intentionally or inadvertently.

Order Now 'The Wuhan Cover-up' by RFK Jr.!

'A Dystopian Solution'

Greg Glaser, J.D., an attorney based in California, told The Defender the proposal is "dystopian." He said:

> "Your human face data is inherently identified with you, meaning if someone sees your face, they know who you are even if they don't know your name. Because your human face image cannot be deidentified for privacy law purposes, tech companies need government authorization to collect and use the data for new uses (or mechanisms) under current privacy law.
>
> "This FTC action under COPPA is another step in the direction of real-time facial recognition monitoring. The companies claim they need to privately examine your child's face and body (yes, the body is viewable with the face) in order to enhance security, but it's a dystopian solution in search of a de minimis problem."

Michael Rectenwald, Ph.D., author of "Google Archipelago: The Digital Gulag and the Simulation of Freedom," told The Defender:

> "The use of facial recognition software, supposedly for verifying users as children, represents a backdoor means for tracking, tracing, and surveilling upon Internet users to unprecedented and hitherto unimaginable degrees.
>
> "It would enable Big Tech to collect biometric information on users, not only to identify them as children (or adults) per se, but precisely as particular individuals."

Derrick Broze, founder and editor-in-chief of The Conscious Resistance Network, said such practices could also lead to the normalization of facial scanning. He said:

> "My major concern is how this technology and others continue to normalize the scanning of faces of those too young to fully grasp the importance of their biometric data.
>
> "Even if Yoti is a trustworthy company this process of scanning your face to verify your age or identity will also help normalize the scanning of faces as a standard way for accessing content."

Along similar lines, Glaser said, "The more regulators open this door to facial surveillance, the more these tech companies will capture faces and bodies not only upon login, but also continuously during product use. They will claim it is necessary to prevent unauthorized access during product use."

California-based attorney Robert Barnes, J.D., said such normalization could, in turn, lead to a normalization of "mass control," telling The Defender:

> "The government seeking to allow companies' biometric testing on kids is the latest effort at mass surveillance. Such surveillance is really about mass control. When has that ever worked out for more freedom for the people rather than less?"

Several of the experts warned there may be other, underlying reasons behind the push for expanded facial recognition and biometric surveillance and warned of potentially harmful consequences for human privacy and anonymity.

Glaser said, "In the bigger picture, there is a sinister reason tech companies desire to openly surveil our faces and bodies while we use their products."

He said:

> "We are normal people, so we naively assume the benign reason is the companies want to enhance their product and service security, but the reality is much darker. Real-time human face data is extremely valuable in conducting AI [artificial intelligence] analysis of human behavior. This is not just for marketing purposes and security. It is for AI development of new products to which we would never consent.
>
> "For example, Facebook is not a charity — they desire to use new AI to convert your family videos into interactive meta experiences they can resell not just to you but to others.
>
> "Bluntly, Facebook's desire is to sell your child's voice and images as 3D experiences that creepy adults enjoy on Meta. And Facebook is not alone in its perversions."

Yoti's website lists Meta — Facebook's parent company — as one of the businesses that "trusts" its products.

According to Rectenwald, "Big Tech companies could thereby establish a biometrically verified identity database replete with precise digital profiles, which could then be used for marketing but also for political, governmental, and other purposes," adding:

> "Given the prevalent sharing of user data between government agencies and Big Tech platforms, these new digital identities would enable the government to undertake precision surveillance, intelligence, and data-collecting operations.
>
> "The last line of online privacy — namely, anonymity — would be utterly eradicated. Also, hackers and other unscrupulous parties could access such data for any number of purposes, including blackmail, extortion, sex and child trafficking, and more."

Along a similar vein, Glaser said that by legalizing such technologies, "regulators are effectively legalizing child porn." He told The Defender:

> "It amazes me that legislators and regulators do not see two steps ahead here to proactively protect children from AI. Tech companies have routinely been caught peddling child pornography uploaded to their sites. Did they reform? No, they are actively becoming surveillance pornographers targeting children.
>
> "With the sheer amount of data they can collect from real-time monitoring of phone and device cameras, together with advanced AI analysis capabilities, regulators are effectively legalizing child porn."

Whistleblowers have previously said that the U.S. government has a poor track record in protecting minors, including from trafficking.

For instance, in April, Tara Lee Rodas, a whistleblower from the U.S. Department of Health and Human Services, said that the U.S. government has become the "middleman" in the transport of unaccompanied minors across the U.S.-Mexico border.

During testimony provided to the House Judiciary Subcommittee on Immigration Integrity, Security, and Enforcement April 26, Rodas said:

> "I thought I was going to help place children in loving homes. Instead, I discovered that children are being trafficked through a sophisticated network that begins with being recruited in their home country, smuggled to the U.S. border, and ends when ORR [Office of Refugee Resettlement] delivers a child to a sponsor — some sponsors are criminals and traffickers and members of Transnational Criminal Organizations."

And Broze warned that despite privacy assurances, policies can later change.

"While it's admirable that Yoti and partners claim they do not store the images of a child's face and do not share the data, history has shown that these corporate policies can change over time," he said.

Age recognition firms connected to Big Tech, BlackRock, government agencies

Yoti, SuperAwesome and Epic Games are also connected to several other major corporations and organizations.

Describing itself as "a digital identity company that makes it safer for people to prove who they are" by "empowering people with a free, reusable digital ID app that minimises the data they share with businesses," Yoti claims it works with "policy advisors, think tanks, researchers, academics, humanitarian bodies, our users and everyday people."

The company also claims it is guided by "seven ethical principles," including "encourag[ing] personal data ownership," "enabl[ing] privacy and anonymity" and "keep[ing] sensitive data secure."

Aside from partnerships with entities such as Meta, the U.K.'s National Health Service, London's Heathrow Airport and the Government of Jersey, Yoti, in 2019, raised 8 million GBP (approximately $10.2 million) from "unnamed private investors."

SuperAwesome, in turn, presents itself as a company providing "Youth marketing solutions" that "powers the youth digital media ecosystem" through "Ads marketplace & gaming solutions," "YouTube & influencer media" and "Parental consent management."

"Youth audiences can't be ignored," the company states. "[As] some of the fastest growing and most engaged digital users, they are a critical audience to drive engagement."

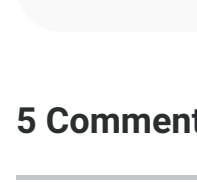
SuperAwesome also promotes youth participation in the metaverse. For instance, one report the company has published, titled "How brands can connect with young audiences in the metaverse," examines "how brands can create branded metaverse content that young people want to see."

Video game developer and retailer Epic Games, SuperAwesome's parent company, has attracted significant corporate investors, including BlackRock, the Walt Disney Company and the Disney Accelerator, Sony and Tencent.

Subscribe to The Defender – It's Free!

First Name.. Last Name.. Email.. SIGN UP

SUGGEST A CORRECTION



Michael Nevradakis, Ph.D.

Michael Nevradakis, Ph.D., based in Athens, Greece, is a senior reporter for The Defender and part of the rotation of hosts for CHD.TV's "Good Morning CHD."

Sign up for free news and updates from Children's Health Defense. CHD focuses on legal strategies to defend the health of our children and obtain justice for those injured. We can't do it without your support.

Republishing Guidelines

Children's Health Defense Comment Policy

We welcome relevant and respectful comments. Off-topic comments may be removed.

Please read our Comment Policy before commenting.

Got it

5 Comments

Login ▾

Join the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name

♡ 7 • Share

Best Newest Oldest

MDskeptic
14 days ago

Allowing government and industry easy access to personal biometric data opens wide the gates of hell. Surveillance, enslavement and dehumanization will quickly follow the adoption of these privacy nullifying technologies.

14 0 Reply • Share ›

Heisenberg
14 days ago

The hypocrisy is multi-layered. 1) They don't care about parental consent when it comes to covid vaccines or gender transition, but video games, now that's a concern. 2) Video games have been violent and sexual for years, but nobody seemed to care before. Remember folks, guns are responsible for school shootings, not our depraved culture and media influence.

How convenient that parental consent is suddenly a selling point now that they're able to deploy their China-like mass surveillance technology. Just look at their investors, that should tell you everything you need to know.

14 0 Reply • Share ›

Classified007
14 days ago edited

Whose to say that this information won't be sold to the government in another blatant overreach attempt to steal data from the public. I don't trust any of these corporations anymore and certainly not the people running the government. Sounds like we need more protections. Time and time again we find blatant overreach occurring. We find illegal databases at the ATF and elsewhere. It's time to drastically reduce federal government size. ATF should be abolished along with the unconstitutional NFA. We need a thorough gutting of FDA, CDC, HHS. Defund NIAD. Any agency that advertises that it's partners with the public sector does not act or perform as proper regulating authority, so dismantle or gut it all. I think a Trump & Kennedy ticket would be ideal for cleaning house.

9 0 Reply • Share ›

Heisenberg → Classified007
14 days ago

They know that the path to ultimate control lies in capturing the children. Once they've got the children, future generations are slaves. And after old-timers like us are gone they'll have no idea what they even lost because history will be re-written. And welcome to the United States of China.

6 0 Reply • Share ›

Gary Brown
14 days ago

Nov 27, 2020 CBP rolls out face biometrics at three additional US points of entry

California and New York pedestrian entry points now equipped with facial recognition.

https://www.biometricupdate...

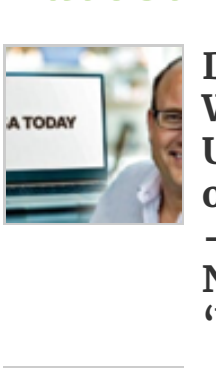
6 0 Reply • Share ›

Subscribe Privacy Do Not Sell My Data

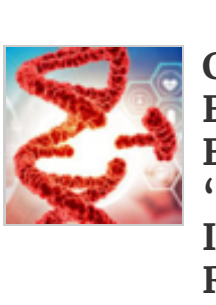
Donate Now
You make the difference.

Latest News

Dr. Pierre Kory: Why We Wrote the USA Today Op-ed on Excess Deaths — and Why We Never Mentioned 'Vaccines'



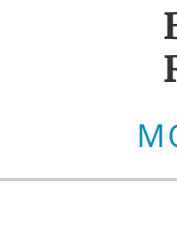
CRISPR Gene Editing: New Evidence of 'Potentially Irreversible Safety Risks'



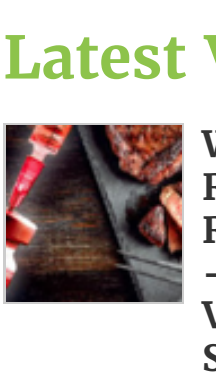
'A Fauci Clone': New NIAID Director Oversaw Remdesivir Trials, Has Ties to Biosafety Lab Research

MORE NEWS

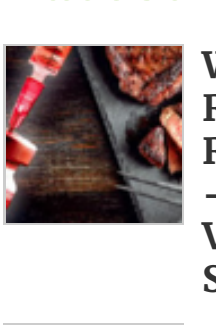
Latest Views



What's Behind the Rapid Spread of Red Meat Allergy — Ticks? Vaccines? Something Else?



Review Adds to Evidence That Glyphosate Weedkillers Cause Cancer



New Book by Doctors for COVID Ethics Details Dangers of mRNA Vaccines

MORE VIEWS

Get FREE News & Updates!

First Name..
Last Name..
Email..
SIGN UP

Children's Health Defense

Children's Health Defense® is a 501(c)(3) non-profit organization. Our mission is to end childhood health epidemics by working aggressively to eliminate harmful exposures, hold those responsible accountable and establish safeguards to prevent future harm. We fight corruption, mass surveillance and censorship that put profits before people as well as advocate for worldwide rights to health freedom and bodily autonomy.

THE DEFENDER IS AVAILABLE IN:
ENGLISH SPANISH PORTUGUESE GERMAN ITALIAN FRENCH

TAKE ACTION
DONATE FREE SIGN-UP BECOME A MEMBER
Donations are tax deductible to the full extent of the law. EIN #26-0388604

Children's Health Defense • Legal Disclaimer • Terms of Use • Privacy Policy • Donate • Work for CHD • Contact • Social

© 2016 - 2023 Children's Health Defense® • All Rights Reserved • Sitemap